MED. INFORM. (1995), VOL. 20, NO. 2, 139–148

Development of security guidelines for existing healthcare systems

S. M. FURNELL, P. W. SANDERS and M. J. WARREN

Network Research Group, Faculty of Technology,
University of Plymouth, Plymouth, UK

(*Received February 1995*)

Abstract. As modern healthcare establishments become increasingly dependent upon information systems it is vital to ensure that adequate security is present to safeguard the confidentiality and integrity of data and the availability of systems. Whilst this is now generally recognized in the design of new systems, many existing operational systems have been implemented without security in mind. This paper describes the need for a standardized approach in the protection of existing healthcare systems within Europe and presents an overview of a new set of information security guidelines that have been developed specifically for the medical community. The guidelines discussed have been produced as a deliverable of the Commission of European Communities (CEC) SEISMED (Secure Environment for Information Systems in Medicine) project, under the Advanced Informatics in Medicine (AIM) programme.

Keywords: Security; Baseline protection; Guidelines; Existing systems.

1. Introduction

The increasing accessibility of information technology (IT) systems during recent years has had a significant effect upon the healthcare field. Many healthcare establishments (HCEs) now operate heterogeneous IT environments with equipment ranging from stand-alone PCs to minicomputer and mainframe installations.

The influence of information systems can now be seen in most areas of healthcare operation, with an ever increasing number and variety of medical applications. In addition, IT also facilitates the exchange of medical data between different HCEs at both national and international levels. A significant result of these advances is that healthcare professionals have become increasingly dependent upon the availability of systems and reliant upon the correctness of the data that they hold.

As the adoption of information technology has increased, so too has the requirement to protect the systems and the information they store. Healthcare systems may be vulnerable to a variety of accidental or deliberate threats and, as such, it is now recognized that security issues must be considered during the development and implementation of new health information systems to maintain the confidentiality, integrity and availability of the data held. Unfortunately, a significant proportion of operational healthcare systems were originally designed and implemented with inadequate security and, as a result, security must also be added or enhanced in many existing systems.

2. The AIM SEISMED project

The issue of information security in healthcare has been addressed by the CEC SEISMED (Secure Environment for Information Systems in Medicine) project, part of the Advanced Informatics in Medicine (AIM) programme [1].

The objective of SEISMED is to provide practical security advice and guidance to all members of the healthcare community who are involved in the management, development, operation or maintenance of information systems. The eventual aim is to establish a consistent framework for the protection of medical data across the European Union.

The project commenced at the beginning of 1992 with an original duration of 3 years, but this was subsequently extended for a further 6 months (until mid-1995). A total of 14 workpackages were established, each addressing a separate aspect of healthcare security. Five European HCEs (located in the UK, The Netherlands, Switzerland and the Czech Republic) were selected to act as *Reference Centres* for the project, commenting upon and ensuring the viability of the recommendations made.

The problem of securing existing systems was addressed by workpackage SP07, the scope of which was to produce a comprehensive set of recommendations for the addition (or enhancement) of security in operational healthcare systems and environments. The principal objectives of this workpackage were:

- to produce guidelines on the level of protection that should be attached to existing operational healthcare systems;
- to provide guidance as to how this level of security may be achieved;
- to revise the approach based upon Reference Centre feedback.

Whilst various guidelines and standards for IT security have previously been developed, none has specifically targeted the needs of the medical community at a European level. The new guidelines are intended to provide a common source of reference for European healthcare establishments and are relevant to (and will affect) all categories of personnel.

3. Baseline security recommendations for healthcare establishments

In order to assess current security practice and attitudes within European establishments a survey was distributed to HCEs in 11 community countries [2]. Amongst other things, this allowed a broad assessment of existing systems to be made and revealed a significant variety in both the types of system in use (i.e. hardware, operating systems and applications) and the levels of security provided. For example, whilst virtually all systems included some form of user authentication mechanism (even if only a simple password in some cases), the attention given to other aspects of security (e.g. disaster recovery, physical protection and auditing) was, in general, significantly less. Furthermore, the variety of techniques used to address a single aspect of protection indicated anything but a standardized approach (e.g. the types of authentication mechanisms variously utilized include individual passwords, shared passwords, challenge–response mechanisms and other methods—with likely inconsistency between similar systems).

It was considered that, in many cases, the disparity indicated by the survey had resulted from the lack of appropriate standards and guidance, with HCEs being unclear over both general security issues and the level they should aim for. The most appropriate strategy for improving the situation was, therefore, considered to be the definition of *baseline* recommendations for security, to provide a common foundation for all HCEs.

This immediately raises the question of what level of security should be specified. The nature of the healthcare environment, with the inherent requirements to

maintain patient safety and confidentiality, demands that protection should generally be higher than in many other domains. As a result, the security requirements extend beyond the levels proposed by many existing standards.

The new baseline recommendations have been developed to satisfy the following aims:

- to represent a minimum acceptable standard for the security of operational healthcare systems and their associated environments;
- to be usable by all HCEs and staff within Europe;
- to allow a straightforward means of validating existing systems security to ensure compliance.

The development of the resulting guidelines was based upon an *interactive* approach, in close co-operation with the SEISMED Reference Centres and in consultation with other independent healthcare professionals.

From the outset it was established that the recommendations should address more than the just the host system in isolation. Indeed to provide comprehensive protection, several aspects of security must be considered:

- logical/system-based controls;
- physical and environmental protection;
- personnel procedures;
- policy and administration issues.

On the basis of these high level requirements, existing IT security guidelines and standards [3–5] were used in conjunction with suggestions from within the project to formulate initial recommendations. These were progressively refined and enhanced over time on the basis of Reference Centre feedback and comments from independent healthcare personnel. This procedure provided the principal criteria for retention, addition or removal of guideline recommendations.

4. An overview of existing systems guidelines

The final *Security Guidelines for Existing Healthcare Systems* [6] are grouped under 10 key *principles* of protection, representing the main elements governing the security of existing healthcare information systems (having been agreed in detail with the Reference Centres). The principles are denoted by ESP followed by a unique reference code, as listed in table 1.

Each of the principles has a number of associated *guidelines*. These represent the

Table 1. Existing systems security principles.

Code	Title
ESP0100	Security policy and administration
ESP0200	Physical and environmental security
ESP0300	Disaster planning and recovery
ESP0400	Personnel security
ESP0500	Training and awareness
ESP0600	Information technology facilities management
ESP0700	Authentication and access control
ESP0800	Database security
ESP0900	System maintenance
ESP1000	Legislation compliance

specific security concepts or countermeasures that should be considered by the HCE to meet the requirements of a given principle. As established earlier, the consideration of existing systems encompasses a very broad range of issues and the overall coverage consequently extends from general concepts to specific technical measures.

The 10 protection principles are described in more detail below. In each case the general purpose of the principle is stated, along with a list of the main issues that are covered by the underlying guidelines (the overall number of guidelines pertaining to each principle is given alongside its title).

4.1. *Security policy and administration (5 guidelines)*

4.1.1. *General principle.* A formal policy will provide clear direction and support for security within the HCE. Policy is formulated from the senior managerial level, with subsequent guidance provided to all levels of staff. Correct administration of and adherence to the policy should ensure the effectiveness of HCE security controls.

4.1.2. *Main issues*

- the need for a security policy;
- policy awareness issues;
- co-ordination and administration of security;
- use of specialist security personnel.

4.2. *Physical and environmental security (22 guidelines)*

4.2.1. *General principle.* The generally open nature of HCEs and their high degree of public access dictates that physical security measures are a vital first stage of protection to prevent unauthorized access to computing equipment and facilities. Systems must also be safeguarded against a variety of environmental hazards that may adversely affect operation.

4.2.2. *Main issues*

- physical access control;
- security of HCE equipment;
- protection against natural disasters;
- environmental controls;
- various procedural measures.

4.3. *Disaster planning and recovery (7 guidelines)*

4.3.1. *General principle.* The continuous availability of Information Systems is essential to the operation of a modern HCE. It is essential that adequate plans are made to ensure the level of availability needed by the HCE can be maintained in the event of any catastrophe. Recovery of IT systems should be a component of an overall HCE disaster/recovery plan.

4.3.2. *Main issues*

- continuity planning (development, testing and update);
- fallback arrangements;
- post-disaster procedures and controls.

4.4. *Personnel security (8 guidelines)*

4.4.1. *General principle.* The major security weakness of many systems is not the technology but the people involved. Many organizations are extremely vulnerable to threats from their own staff and, as a result, even the most comprehensive technical controls will not guarantee absolute security. There are, however, a number of personnel-related measures that can be introduced to help reduce the risks.

4.4.2. *Main issues*

- staff recruitment;
- contractual agreements promoting security;
- security during normal working practices;
- staff appraisal and monitoring;
- termination of employment.

4.5. *Training and awareness (6 guidelines)*

4.5.1. *General principle.* Information systems security can only be maintained if all personnel involved in their use know, understand and accept the necessary precautions. Many breaches are the result of incorrect behaviour by general staff who are unaware of security basics. The provision of security training and awareness will make it possible for staff to consider the security implications of their actions and avoid creating unnecessary risks.

4.5.2. *Main issues*

- the need for general security awareness;
- specific areas that must be addressed (job training, use of information systems);
- recommendations for internal/HCE training and awareness initiatives;
- use of specialist training courses;
- assignment of responsibilities for training.

4.6. *Information technology facilities management (31 guidelines)*

4.6.1. *General principle.* A variety of activities can be identified that are related to the normal day-to-day use and administration of information systems. All categories of HCE personnel (management, technical and general users) have responsibilities that must be addressed in order to maintain security in this area.

4.6.2. *Main issues*

- system planning and control;
- the importance of maintaining back-ups;
- media controls;
- auditing and system monitoring;
- virus controls;
- documentation issues.

4.7 *Authentication and access control (28 guidelines)*

4.7.1. *General principle.* It is essential that IT systems are protected by comprehensive logical access controls. Access should be guaranteed for legitimate users and denied to all others. *All* classes of user must be identified and authenticated before *any* access is granted and further mechanisms must control subsequent reading, writing, modification and deletion of applications and data. There should be no method for bypassing any authentication or access controls. HCE users are unlikely to be satisfied with controls that intrude upon working practices, and chosen schemes should be transparent and convenient in order to gain acceptance.

4.7.2. *Main issues*

- requirements for user identification and authentication;
- password issues;
- system and object access restrictions;
- methods of control;
- access in special cases (e.g. system management, third parties, temporary staff).

4.8. *Database security (21 guidelines)*

4.8.1. *General principle.* Database security is concerned with the enforcement of the security policy concerning the disclosure, modification or destruction of a database system's data. Databases are fast becoming very important for HCEs. Over 90% of today's IT systems contain some kind of database and the value of information stored is now widely recognized as a major asset, far more important than any software. However, databases also introduce additional security concerns (e.g. granularity, inference, aggregation, filtering, journaling, etc.) and therefore warrant specific consideration.

4.8.2. *Main issues*

- control of medical database software;
- organization and administration of HCE database systems;
- database operation issues.

4.9. *System maintenance (5 guidelines)*

4.9.1. *General principle.* System maintenance activities merit special consideration given the opportunities that exist to affect the operation of the system. Unauthorized or uncontrolled changes to any aspect of an operational system could potentially compromise security and, in some cases, endanger life. Maintenance must therefore be carried out in accordance with well-defined procedures.

4.9.2. *Main issues.*

- controls to prevent unauthorized changes to and upgrades of HCE software, vendor software and operating systems;
- requirements for testing and acceptance.

4.10. *Legislation compliance (5 guidelines)*

4.10.1. *General principle.* Specific levels of protection may be demanded in order to comply with national and European legislative requirements, as well as to satisfy internal HCE policy. Whilst the guidelines highlight the most basic requirements, this principle represents an ongoing process which must take account of any new legislation that may be relevant, as well as ensuring compliance with existing standards.

4.10.2. *Main issues*

- data protection;
- abuse of information systems;
- compliance with internal security standards;
- retention and protection of business records.

5. HCE target audiences

It should be evident that many of the issues covered are not relevant to all HCE staff. As such, the *Security Guidelines for Existing Healthcare Systems* are targeted at three main staff groups (as shown in figure 1), with separate guideline sets having been developed for each audience. Whilst all three sets draw upon the same core principles, they nevertheless differ dramatically in terms of the type and quantity of information presented. The anticipated readership and general content of each set is as follows:

- The *General* guideline set is aimed at the majority of HCE staff, including clinicians, administrators and general system users. Guidelines are presented for user reference during day-to-day use of HCE information systems, highlighting what they can do to safeguard security.
- The *Management* set primarily targets the senior decision makers within the HCE, who will be responsible for defining security policy (although a significant number of points will also be relevant at department/line management level). This set is intended to highlight areas in which management should be directly involved and also improve management security awareness by explaining/justifying the importance of other more technical guidelines (for which management approval will be required).

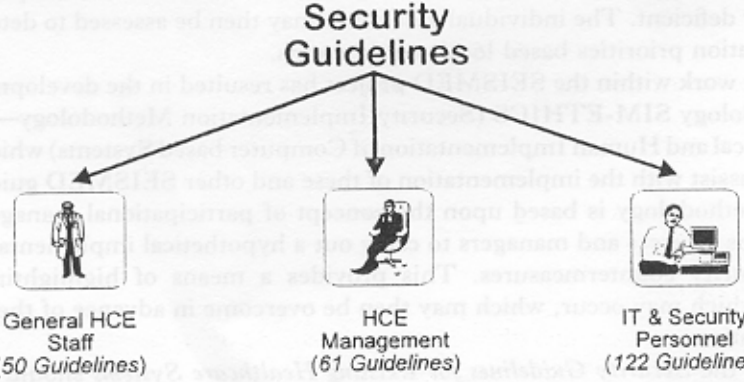

Figure 1. HCE target audiences.

- The *IT and Security Personnel* set is aimed at IT staff, system administrators, security officers and other support staff who will be most likely to have the lower level responsibilities for implementing security. This is the most detailed of the subsets and should be a key source of reference for implementation and validation of security.

The *Management* and *IT and Security* audiences would also be expected to read and observe the *General* guideline set.

6. Implementing the recommendations

The *Security Guidelines for Existing Healthcare Systems* should be applied in any European Healthcare Establishment with existing operational information systems (where the term *Healthcare Establishment* refers to any establishment providing medical services, research, training or health education). They will be relevant even where systems are thought to include security provision, so that the level of protection can be validated against the recommendations.

However, given the diverse nature of European healthcare environments and systems, it is impossible to specify precise guidelines for implementation. Establishments will differ in terms of both the information systems used, as well as financial, operational and other constraints that may apply. These issues will all have bearing on the applicability of the recommendations. The guidelines therefore concentrate more on describing *what* aspects of security should be considered rather than *how* they may be best implemented (with broad recommendations that should be compatible, to at least some degree, with the majority of systems and environments).

Despite these attempts to ensure applicability, it is still conceivable that some guidelines may not be suitable for all systems. As such, implementors must use their discretion in cases where guidelines are genuinely inappropriate to the environment. However, recommendations should be followed as closely as possible and in some cases the implementation of a guideline *will* depend upon others already being in place (which is made clear from the guideline context and/or cross-references to other points).

As for the implementation strategy itself, it would obviously be impractical to attempt to address all of the suggestions at once due to constraints of cost and likely disruption to services. A phased approach is, therefore, advised in which each principle is considered in turn to identify the areas in which the HCE/department is currently deficient. The individual guidelines may then be assessed to determine implementation priorities based local requirements.

Further work within the SEISMED project has resulted in the development of the methodology SIM-ETHICS (Security Implementation Methodology—Effective Technical and Human Implementation of Computer based Systems) which may be used to assist with the implementation of these and other SEISMED guidelines [7]. The methodology is based upon the concept of participational management, using groups of users and managers to carry out a hypothetical implementation of chosen security countermeasures. This provides a means of highlighting any problems which may occur, which may then be overcome in advance of the actual implementation.

Finally, the *Security Guidelines for Existing Healthcare Systems* should not be considered in isolation and a number of other SEISMED guideline deliverables are

also relevant in the context of existing systems. These include specific guidelines relating to high-level security policy, system development and implementation, network security and data encryption.

7. Potential problems

Whilst the new recommendations are intended tc provide a simple and straightforward means of addressing healthcare security issues, it is recognized that problems may exist.

Firstly, many establishments may currently be operating with security significantly below the recommended level and progression to the required level may be a non-trivial task. As mentioned in the discussion of implementation, HCEs may face a number of constraints that affect their ability to address security requirements. For example, cost (in terms of finance, performance and practicality) will be a significant factor in determining acceptability. Financial cost will be particularly relevant, given that expenditure for direct care activities is likely to receive higher priority than security. In addition, organizational constraints will play a role in so far as recommendations will need to integrate with existing practice (or at least not conflict too greatly) in order to gain acceptance. If such constraints are present, establishments should bear in mind that every guideline implemented will improve the security of their systems.

Conversely, some environments and/or applications may demand a level of security significantly higher than the proposed baseline. In these cases a risk analysis review is recommended in order to determine the level of additional protection that is necessary. A specifically designed healthcare protection methodology, that has also been developed by this group, could be utilized for this purpose [8].

8. Conclusions

In conclusion, it is believed that the guidelines have fulfilled the objectives of this phase of the SEISMED project and will provide a solid foundation for the improvement of security within existing HCE systems.

Whilst the principles will remain relatively static, it is expected that the underlying guidelines will require periodic updates to account for changes within the healthcare field or in the types of information system technology available (e.g. the increasing use of multimedia systems may introduce new considerations). Changes within the local HCE (e.g. organizational structure, medical applications and practices) may also necessitate re-evaluation of some recommendations.

The guidelines will now form the basis of a further SEISMED workpackage dedicated to the validation of the project's recommendations. This will include full trials of the guidelines at the Reference Centres and will provide an extensive test of their applicability in practice. It is anticipated that the Reference Centres themselves will then be able to document their findings in due course.

Acknowledgements

We would like to acknowledge the various partners and collaborators within the SEISMED project for their valuable contributions during the development of these guidelines. In particular, we would like to thank the following individuals for their help and assistance throughout the project: Dr Barry Barber (NHS Information Management Centre, United Kingdom); Mr John Fowler (Royal London Hospital, United Kingdom); Dr Nick Gaunt (Plymouth Health Authority, United Kingdom),

Dr Kees Louwerse (Leiden University Hospital, The Netherlands), Prof. George Pangalos (University of Thessaloniki, Greece).

References

1. AIM SEISMED PROJECT (1991)Technical Annex. Secure Environment for Information Systems in MEDicine. SEISMED (A2033).
2. AIM SEISMED PROJECT (1995) Enhanced Survey Report. Deliverable 34. Secure Environment for Information Systems in MEDicine. SEISMED (A2033).
3. CCTA (1993) Baseline Security for IT Systems. (June.).
4. DEPARTMENT OF TRADE & INDUSTRY (1993) A Code of Practice for Information Security Management. (Sept.).
5. NHS MANAGEMENT EXECUTIVE INFORMATION MANAGEMENT GROUP (1992) Basic Information Systems Security.
6. AIM SEISMED PROJECT (1994) Security Guidelines for Existing Healthcare Systems. Deliverable 26. Secure Environment for Information Systems in MEDicine SEISMED (A2033).
7. WARREN, M. J., and GAUNT, P. N., (1993) Impact of security on a healthcare environment and how to overcome it. In *Proceedings of IMIA Working Conference on Caring for Health Information*, 13–16 November (Heemskerk, The Netherlands).
8. FURNELL, S. M., GAUNT, P. N., PANGALOS, G., SANDERS, P. W., and WARREN, M. J., (1995) A generic methodology for health care data security. *Medical Informatics*, **19**, 229–246.